NASA New Approach for Evaluating Risk Reduction Due to Space Shuttle Upgrades

Fayssal M. Safie, Ph.D. • NASA • Huntsville
Rebecca L. Belyeu • Hernandez Engineering Inc. (HEI) • Huntsville

Key Words: Quantitative Risk Assessment, Space Shuttle, Redesign

SUMMARY & CONCLUSIONS

As part of NASA's intensive effort to incorporate quantitative risk assessment (QRA) tools in the Agency's decision-making process concerning Space Shuttle risk, NASA has developed a powerful risk assessment tool called the Quantitative Risk Assessment System (QRAS). The QRAS is a tool designed to estimate Space Shuttle risk and evaluate Space Shuttle upgrades. This paper presents an overview of the QRAS with focus on its application for evaluating the risk reduction due to proposed Space Shuttle upgrades. The application includes a case study from the Space Shuttle main engine (SSME).

The QRAS overview section of the paper includes the QRAS development process, the technical approach to model development, the QRA quantification methods and techniques, and observations concerning the complex modeling involved in QRAS. The application section of the paper describes a practical case study using QRAS models for evaluating critical Space Shuttle Program upgrades, specifically a proposed SSME nozzle upgrade. This paper presents the method for evaluating the proposed upgrade by comparing the current nozzle (old design with well-established probabilistic models) to the channel wall nozzle (new design at the preliminary design level).

1. INTRODUCTION

Since the Space Shuttle Challenger accident in 1986, NASA has begun incorporating QRA in decisions concerning the Space Shuttle and other NASA projects. At Marshall Space Flight Center (MSFC), for example, QRA has been extensively used in areas such as risk management of flight hardware, trade studies, and reliability prediction of new hardware. In the risk management area, life limits based on QRA are being used in the SSME program (Ref. 1). QRA has also been incorporated to support flight issues on the SSME as well as other MSFC elements. With regard to trade studies, QRA has been used as the basis to evaluate the elimination of unnecessary inspections, procedures, and other program costs. For example, an extensive study was conducted in 1994 to determine whether to eliminate the preproof test x-ray inspections on the Space Shuttle external tank (ET) (Ref. 2). In the reliability prediction area, similarity analysis and probabilistic structural models have been used by MSFC to predict the reliability of newly developed hardware such as X–33 and X–34 engines. Such models are discussed in Ref. 3. In addition to the ongoing QRA effort at the various NASA centers, NASA Headquarters has led several studies to predict the overall Space Shuttle risk. These studies are the most extensive QRA studies that have been conducted by NASA. The first of these Space Shuttle QRA studies was conducted in 1988 by Planning Research Corporation (PRC). Per NASA's request, PRC conducted a QRA study to determine the Space Shuttle risk for the Galileo mission (Ref. 4). In 1993, Science Applications International Corporation (SAIC) updated the Galileo study using Bayesian techniques (Ref. 5). In 1995, SAIC conducted a comprehensive QRA study (Ref. 6). In July 1996, the NASA Administrator requested an independent QRA to be conducted by NASA QRA experts. Before July 1996, all the QRA studies performed on the Space Shuttle system had been conducted by independent consultants outside of NASA. In response to the Administrator's request, NASA is conducting a study to develop a model that will provide an overall Space Shuttle risk and estimates of risk changes due to proposed Space Shuttle upgrades. The development of the model consists of two major efforts. One is the development of the risk model and the other is the development of the computer software to run the model. The risk model is being developed by MSFC and Johnson Space Center (JSC) and the computer software, QRAS, is being developed by NASA Headquarters.

This paper presents an overview of the QRAS with focus on its application for evaluating the risk reduction due to proposed Space Shuttle upgrades. The application includes a case study from the SSME. This case study represents NASA's new approach for evaluating risk reduction due to Space Shuttle upgrades.

2. QRAS OVERVIEW

2.1 *QRAS Development Process*

The QRA strategy for conducting the QRAS project focused on a team approach. The team approach involved both Government and industry, with team members representing various technical disciplines. This includes design engineers, safety engineers, statisticians, and QRA experts. The QRA team approach has proven to be very effective in capturing the knowledge, data, and expertise required in conducting a complex task such as the Space Shuttle QRA study. This approach has

also proven to facilitate the customer buy-in and improve the fidelity of the analyses results.

2.2 *QRAS Technical Approach*

The first step in the QRAS technical approach is the identification of the most critical failure modes or events to be modeled. This can be accomplished using various methods. One method is using a master logic diagram (MLD) as shown on the upper left-hand side of Figure 1. The MLD is basically a fault tree with its basic events being the failure modes/causes to be modeled. Other methods involve using failure modes and effects analyses (FMEA) and hazard analyses combined with screening criteria to identify the most critical failure modes/causes to be modeled. In QRA terminology, the identified failure modes/causes are called initiating events.

The second step in the QRAS technical approach is the development of an event sequence diagram (ESD) for each initiating event identified in Step 1. The ESD shown in Figure 1 describes how failures could propagate through the system along various scenarios leading to mission success, loss of vehicle/crew, or other end states; or how mitigating factors could prevent the initial failure from propagating to undesirable end states, thereby protecting the higher level system. Note that a circle represents an initiating event, a rectangle represents a pivotal event, a parallelogram represents a comment, and a diamond represents an end state.

The third step in the QRAS technical approach is to translate each ESD to an event tree to determine the probability of Space Shuttle failure due to the ESD initiating event. The event tree probabilities require the quantification of the initiating and pivotal events (described in Section 2.3).

The final step in the QRAS technical approach is to aggregate the probabilities of all initiating events to obtain the probability of catastrophic failure at the failure mode, component, subsystem, element, and Space Shuttle level.

The above-described approach is based on fault trees, ESDs, and event trees. Although QRAS uses logic trees, which have historically been used in all large-scale QRA studies, the application of these tools and the quantification methods used in QRAS approach are different. For instance, in order to be able to evaluate Space Shuttle upgrades, all logic trees used in this study are developed with a high level of modularity. In the quantification area, advanced probabilistic structural models (Refs. 7–9) are extensively used to account for lack of data, especially when modeling redesigned hardware.

2.3 *Quantification Methods and Techniques*

The quantification of the initiating and pivotal events in the above discussion is done in two steps. The first step is establishing a failure distribution for the initiating/pivotal events. The second step is establishing an uncertainty distribution on the probability of failure. The most commonly used models for

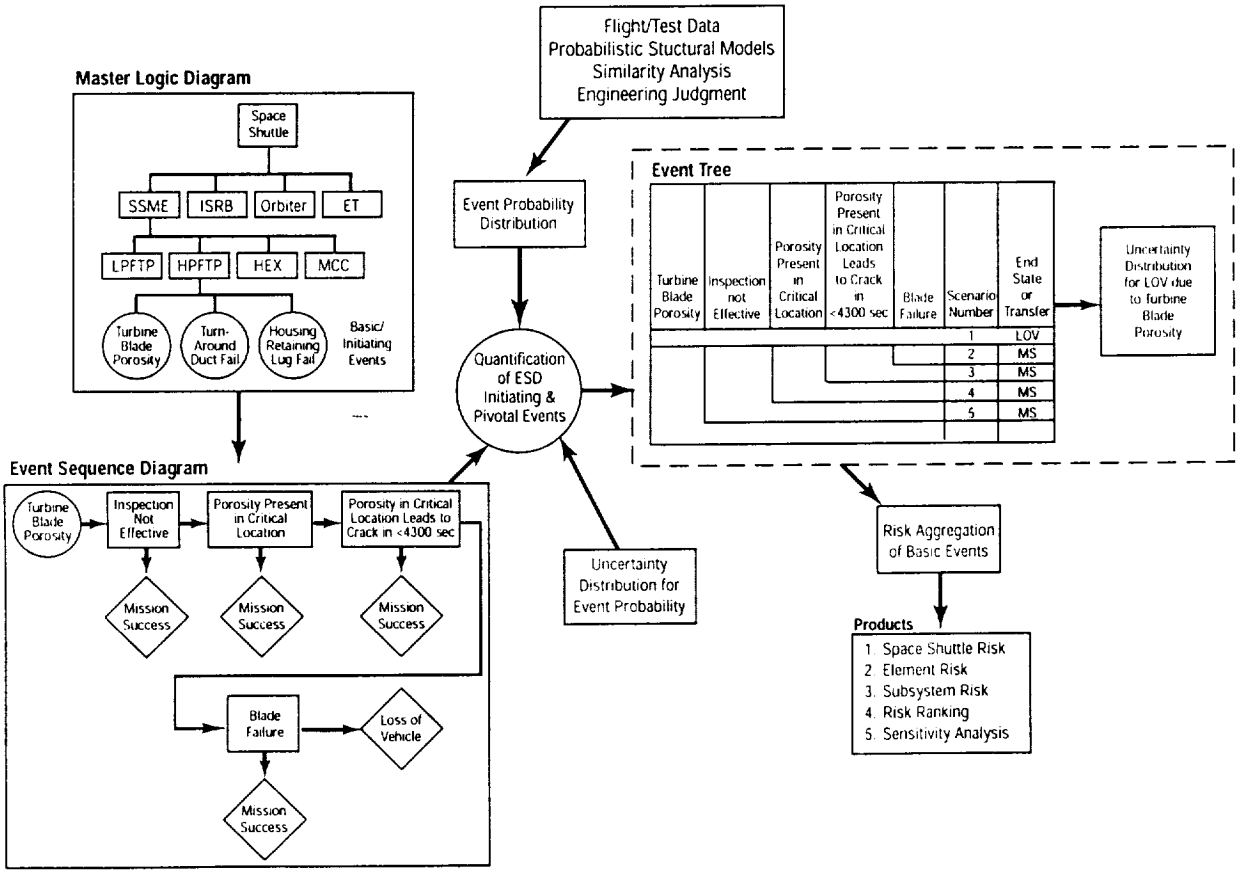

Figure 1. QRAS Technical Approach

characterizing failure distributions are Binomial, Exponential, Weibull, Lognormal, Normal, and reliability growth. The selection of the distribution depends on the nature of the failure and the data. Numerical/frequency distributions can also be used to characterize the failure distribution where failures are generated by simulation. With regard to the uncertainty distribution on the probability of failure, the most commonly used distributions are the Lognormal, Weibull, and the Beta distribution. Since validation of an uncertainty distribution is difficult, in most cases, the selection of the uncertainty distribution is arbitrary.

2.4 *Key Observations*

From the above discussions, it is observed that the quantification of the initiating and pivotal events requires a large amount of data given all the failure modes that need to be modeled in the Space Shuttle study. This, in some cases, has the potential to be a problem. However, this data problem can be overcome by using similarity analysis, engineering models such as probabilistic structural models (Ref. 7), and by utilizing good engineering judgement. The effect of lack of data can also be minimized by the one-time construction of a well documented, maintainable, "living" model that can be easily updated as more data become available.

It is also observed that successful QRA studies require a well-defined, documented, and systematic procedure, and also assembling the right team including design and systems engineers. In fact, the high level of success of this NASA led QRA study is attributed to the process followed in conducting the study, the participation of various disciplines, and the use of all Space Shuttle generated data including test, flight and engineering analyses.

3. A CASE STUDY USING QRAS FOR EVALUATING UPGRADES

The SSME is a very complex propulsion element, both in the design and the operating environment. As a result, the operational reliability for such a system is very critical for a safe and successful launch of the Space Shuttle. One of the critical components of the SSME is the nozzle. The following sections address a case study, which involves the application of QRAS to evaluate the risk reduction due to redesign of the SSME current tube nozzle. The new design evaluated is the channel wall nozzle (CWN).

3.1 *Current SSME Nozzle Description—Tube Nozzle*

The SSME nozzle increases the velocity of the exhaust gas stream by controlling its expansion and attendant pressure reduction. Optimum expansion, as well as maximum thrust, exist when gas pressure at the nozzle exit plane equals ambient pressure. The nozzle consists of 1,080 stainless steel tubes brazed to themselves and to a surrounding structural jacket. Nine hatbands are welded around the jacket for hoop strength. Coolant manifolds are welded to the top and bottom of the nozzle, along with three fuel transfer ducts and six drain lines. Figure 2 shows the current SSME tube nozzle.

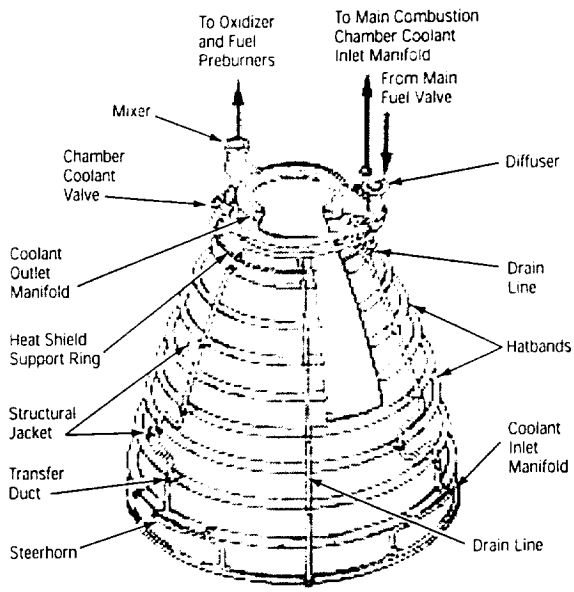

Figure 2. SSME Tube Nozzle

3.2 *Channel Wall Nozzle Design*

The CWN is a simplified nozzle design with fewer parts than the tube nozzle described above. The details of the CWN design are proprietary; hence, the information given here is not specific or detailed. The CWN design mainly addresses the highest risk failure modes of the current design; two of which are contamination blockage and structural failure due to fatigue, e.g. feedlines. With regard to contamination, the individual tubes of the tube nozzle are replaced by milled channel/jacket assembly in the CWN design. Channels are larger and are expected to have less blockage compared to particle sizes that are blocking the tube nozzle. Even in the case of blockage, the channel would be only partially blocked. In addressing structural failure due to fatigue, the CWN design places the feedline inlet at the midsection of the nozzle. This change translates to a significant reduction in transient load over the tube nozzle.

3.3 *Risk Reduction of the Tube Nozzle Versus Channel Wall Nozzle Evaluation and Results*

The process of evaluating the risk reduction of the CWN involved identifying the critical failure modes/causes, developing ESDs, and assessing the high-risk items using QRAS where information is available. Failure mode identification revealed that both nozzles have the same catastrophic failure modes, which are internal and external leakage of hydrogen. Following the failure mode identification, high-risk failure modes were assessed as follows. First, ESDs were developed for all critical failure modes under consideration. Second, the ESDs were assessed quantitatively/qualitatively for major risk reductions. The high-risk failure

modes evaluated involved nozzle failure due to contamination blockage and structural failure due to fatigue, e.g. feedlines. The evaluation was conducted using the current nozzle-existing QRAS models as the baseline. The design changes in the CWN were then evaluated for risk reduction compared to the baseline. An example model of the QRAS application is depicted in the ESD shown in Figure 3.

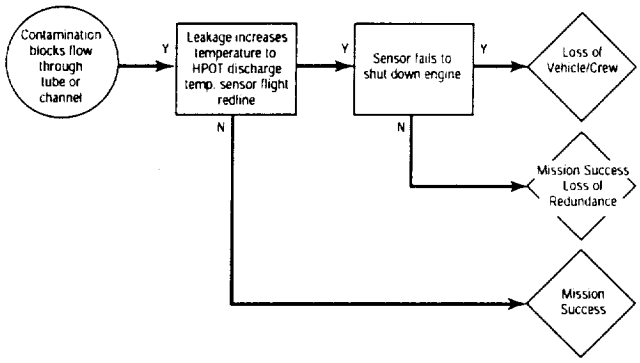

Figure 3. Example ESD

It is important to note that the ESD in the above example is the same for both nozzle designs with the exception of the quantification of the initiating event. The probability for the initiating event for the CWN is based on channel blockage, while for the tube nozzle, the probability is based on blockage of the tubes. Since channels are larger than the tubes, the probability of contamination blockage for the CWN is expected to be lower. Similarly, structural failures due to fatigue, along with other failure modes, were evaluated for risk reduction.

In addition to evaluating the risk reduction due to design improvements, new failure modes introduced by the CWN design were also evaluated.

Results of the study indicated that although the CWN showed that significant risk reductions could be obtained, the introduction of new failure modes could play a key role in the final decision.

4. CONCLUDING REMARKS

We have presented the methodology and application of the tool that NASA has developed to evaluate the Space Shuttle risk at various levels—system, subsystem, component, and failure mode. Although the tools have been successfully used to evaluate risk reduction due to Space Shuttle upgrades, it is important to keep in mind that evaluating risk reduction due to proposed upgrades might require extensive engineering involvement. Specifically, since a proposed upgrade lacks the data required to develop QRAS-type models, the evaluation process is highly dependent on engineering judgement/ assessment. Engineering assessment is required to determine the level of risk reduction by evaluating the impact of the design changes on the risk of the current design which has well-established QRAS models.

REFERENCES

1. F.M. Safie, "A statistical approach for risk management of Space Shuttle main engine components", *Probabilistic Safety Assessment and Management*, 1991.
2. F.M. Safie, "A risk assessment methodology for the Space Shuttle External Tank welds", *Reliability and Maintainability Symposium*, 1994.
3. F.M. Safie, "Use of probabilistic design methods for NASA applications", *ASME Symposium on Reliability Technology*, 1992.
4. Planning Research Corporation, "Independent assessment of Shuttle accident scenario probabilities for Galileo mission and comparison with NSTS program assessment", 1989.
5. Science Applications International Corporation, "Probabilistic risk assessment of the Space Shuttle phase I: Space Shuttle catastrophic failure frequency final report", 1993.
6. Science Applications International Corporation, "Probabilistic risk assessment of the Space Shuttle", 1995.
7. C.R. Hoffman, R. Pugh, F.M. Safie, "Methods and techniques for risk prediction of Space Shuttle upgrades", *AIAA*, 1998.
8. E.P. Fox, "SSME alternate turbopump development program—probabilistic failure methodology interim report", *FR-20904-02*, 1990.
9. F.M. Safie, E.P. Fox, "A probabilistic design analysis approach for launch systems", *AIAA/SAE/ASME 27th Joint Propulsion Conference*, 1991.

BIOGRAPHIES

Fayssal M. Safie, *Ph.D., CRE*
NASA/QS10
George C. Marshall Space Flight Center (MSFC)
Marshall Space Flight Center, AL 35812 USA

Internet (e-mail): fayssal.safie@msfc.nasa.gov

Fayssal Safie is a lead reliability and quality engineer at MSFC. Before joining MSFC in 1986, he served as a visiting assistant professor at Cleveland State University. Besides his responsibility at MSFC, Dr. Safie is serving as an Adjunct Professor at the University of Alabama in Huntsville (UAH). At MSFC, he is serving as "Man in the Job" for all statistical analyses conducted throughout the Center. In 1988, Dr. Safie received the NASA Exceptional Engineering Achievement Medal for his contribution to the "Space Shuttle Return to Flight" effort. In 1995, he received the NASA Quality Excellence Award for being selected as the "Best of the Best" throughout all NASA centers in the Safety, Reliability, and Quality Assurance area. In 1998, he received an award for Flight Safety Awareness for his significant contribution to the NASA Quantitative Risk Assessment System. Dr. Safie received his Ph.D. from Cleveland State University. He is a member of ASQC and a senior member of AIIE.

Rebecca L. Belyeu
Hernandez Engineering Inc. (HEI)
George C. Marshall Space Flight Center
Marshall Space Flight Center, AL 35812 USA

Internet (e-mail): becky.belyeu@msfc.nasa.gov

Ms. Belyeu is a reliability engineer in HEI's Reliability and Maintainability Engineering Group on the MSFC Safety and Mission Assurance contract. Ms. Belyeu has extensive work experience in the areas of reliability predictions, quantitative risk assessments, and reliability/maintainability analysis. She has a Bachelor of Science degree in Mathematics and Computer Science from Jacksonville State University. Ms. Belyeu has been given several NASA awards for her contribution to the space program.